

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-260640

(43)Date of publication of application : 16.09.2004

(51)Int.Cl.

H04L 9/32

(21)Application number : 2003-050248

(71)Applicant : HITACHI LTD

(22)Date of filing : 27.02.2003

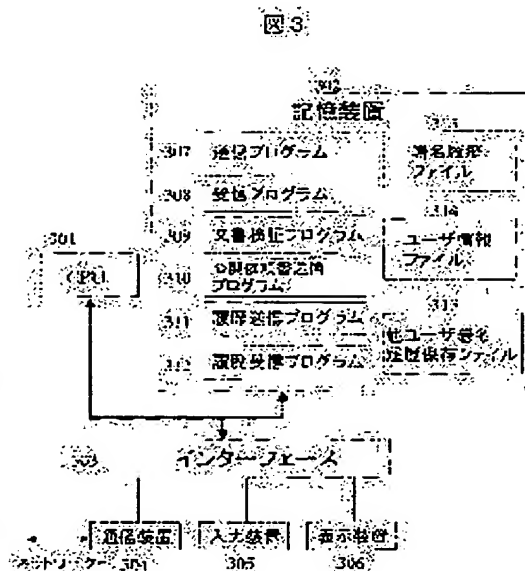
(72)Inventor : TANIMOTO KOICHI  
MIYAZAKI KUNIIHIKO  
ITO SHINJI  
KUDO YASUAKI  
BESSHO RYOJI

## (54) METHOD AND DEVICE FOR DISCLOSING SIGNATURE RECORD

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a disclosure system which is for a public organization and is efficient and secure to the public organization and to provide a user with a signature verification function that uses a disclosed signature record.

**SOLUTION:** This public organization discloses a signature record received from a user to a Web. When the public organization opens the signature record, the public organization acquires a time stamp and returns the time stamp to the user as well as disclosure notification. The public organization has a signature history and periodically discloses a portion of the history to newspapers, etc. Otherwise, the public organization prepares data for disclosure on the basis of a signature record received from each user and discloses the data to the newspapers. The public organization transmits the signature history of the public organization to the user after disclosing the data to the newspapers.



## LEGAL STATUS

[Date of request for examination]

07.02.2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-260640

(P2004-260640A)

(43) 公開日 平成16年9月16日(2004. 9. 16)

(51) Int. Cl. <sup>7</sup>

H04L 9/32

F1

H04L 9/00

675Z

H04L 9/00

675B

テーマコード(参考)

5J104

審査請求 未請求 請求項の数 14 O L (全 21 頁)

(21) 出願番号 特願2003-50248 (P2003-50248)

(22) 出願日 平成15年2月27日(2003. 2. 27)

(出願人による申告) 国等の委託研究の成果に係る特許出願(平成14年度通信・放送機構「次世代証拠基盤技術に関する研究開発」委託研究、産業活力再生特別措置法第30条の適用を受けるもの)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(74) 代理人 100075096

弁理士 作田 康夫

(72) 発明者 谷本 幸一

神奈川県川崎市麻生区王禅寺1099番地

株式会社日立製作所システム開発研究所内

(72) 発明者 官崎 邦彦

神奈川県川崎市麻生区王禅寺1099番地

株式会社日立製作所システム開発研究所内

最終頁に続く

(54) 【発明の名称】 署名記録の公開方法、および装置

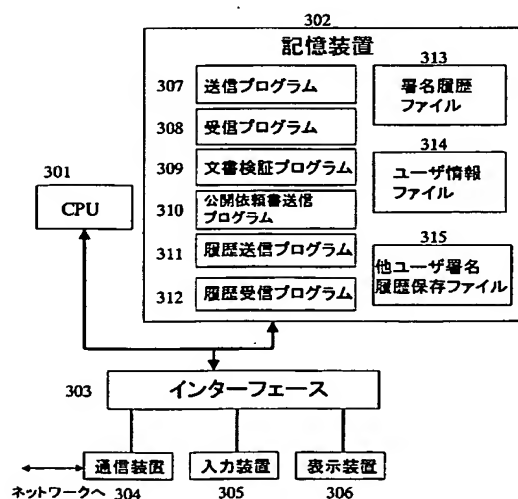
(57) 【要約】

【課題】 公開機関のための、公開機関およびユーザにとって効率的で安全な公開システムと、ユーザに対して、公開された署名記録を利用した署名検証機能を提供する。

【解決手段】 公開機関は、ユーザから受け取った署名記録をWebに公開する。公開時にはタイムスタンプを取得し、公開通知書とともにユーザに返信する。公開機関も署名履歴を持ち、履歴の一部を定期的に新聞等に公開する。もしくは、各ユーザから受け取った署名記録を基に公開用データを作成し、それを新聞に公開する。公開機関は、新聞公開後に公開機関の署名履歴をユーザに送信する。

【選択図】 図3

図3



## 【特許請求の範囲】

## 【請求項 1】

ユーザ側装置が生成した署名に関わる情報を記録した署名記録の公開方法であって、  
公開機関側装置において、  
前記ユーザ側装置が作成したユーザ署名記録を受信し、公開するユーザ署名記録公開ステップと、  
前記ユーザ署名記録を公開したことを、前記ユーザに通知するユーザ署名記録公開通知ステップと、  
受信した前記ユーザ署名記録を用いた公開機関署名記録を作成し、過去に作成した公開機関署名記録が登録されている署名履歴を更新する署名履歴更新ステップと、  
作成した前記公開機関署名記録を公開する公開機関署名記録公開ステップと、  
前記公開機関署名記録を公開したことを前記ユーザに通知する公開機関署名記録公開通知ステップと、を有する  
ことを特徴とする署名記録の公開方法。

10

## 【請求項 2】

請求項 1 記載の署名記録の公開方法であって、  
前記署名履歴更新ステップは、  
前記公開機関署名記録を、受信した前記ユーザ署名記録と、複数の他の署名記録に基づいて作成し、署名履歴ファイルに記録する署名記録作成ステップと、  
前記ユーザに関わる情報と受信した前記ユーザ署名記録に関する情報をユーザ情報ファイルに記録するユーザ情報ファイル更新ステップと、からなる  
ことを特徴とする署名記録の公開方法。

20

## 【請求項 3】

請求項 1 記載の署名記録の公開方法であって、  
前記ユーザ署名記録公開ステップは、  
前記ユーザ署名記録の公開日時を保証するタイムスタンプを取得するタイムスタンプ取得ステップを有する  
ことを特徴とする署名記録の公開方法。

## 【請求項 4】

請求項 2 記載の署名記録の公開方法であって、  
前記署名記録作成ステップは、  
前記ユーザ署名記録について、署名アルゴリズム識別情報と、署名記録固有に付けられる署名番号と、連鎖の検証に利用する前回署名記録のハッシュ値と、受信した前記ユーザ署名記録の署名番号とハッシュ値と、からなる前記公開機関署名記録を作成し、  
前記署名履歴に新たに作成した前記公開機関署名記録を追加する  
ことを特徴とする署名記録の公開方法。

30

## 【請求項 5】

請求項 2 記載の署名記録の公開方法であって、  
前記ユーザ情報ファイル更新ステップは、  
前記公開機関署名記録に付けられた署名番号と、  
対応する前記公開機関署名記録がユーザ署名記録の受信に応じて作られたことを示す受信符号と、  
前記ユーザ署名記録の送信者を示す相手情報と、  
受信したユーザ署名記録に付けられた署名番号と、  
受信した前記ユーザ署名記録と、  
からなるデータを作成して、前記ユーザ情報ファイルに追加する  
ことを特徴とする署名記録の公開方法。

40

## 【請求項 6】

請求項 1 記載の署名記録の公開方法であって、  
前記公開機関側装置のユーザ署名記録公開通知ステップは、

50

公開したことを前記ユーザ側装置のユーザに通知するための公開通知書を作成する公開通知書作成ステップと、  
作成した前記公開通知書と前記署名履歴中の前回署名記録から署名を作成し、前記公開通知書に添付する署名作成ステップと、  
作成した署名の情報を前記署名履歴に記録する署名履歴更新ステップと、  
前記ユーザに関わる情報を前記ユーザ情報ファイルに記録するユーザ情報ファイル更新ステップと、  
作成した前記公開通知書を前記ユーザに送信する送信ステップと、からなることを特徴とする署名記録の公開方法。

【請求項 7】

請求項 6 記載の署名記録の公開方法であって、  
前記公開通知書作成ステップは、  
公開したことを前記ユーザに伝える文書と、  
公開した公開署名記録と、  
公開した日時を伝えるタイムスタンプと、  
に基づいた公開通知書を作成することを特徴とする署名記録の公開方法。

【請求項 8】

請求項 6 記載の署名記録の公開方法であって、  
前記署名履歴更新ステップは、  
署名アルゴリズム識別情報と、  
署名記録固有に付けられる署名番号と、  
連鎖の検証に利用する前回署名記録のハッシュ値と、  
署名作成対象文書のハッシュ値と、  
作成した署名と、  
とからなる署名記録を作成し、前記署名履歴に追加することを特徴とする署名記録の公開方法。

【請求項 9】

請求項 6 記載の署名記録の公開方法であって、  
前記ユーザ情報ファイル更新ステップは、  
署名記録と関連付けられた署名番号と、  
対応する公開機関署名記録が署名作成時に作られたことを示す符号と、  
前記公開通知書を送信する前記ユーザを示す相手情報と、  
からなる情報を前記ユーザ情報ファイルに追加することを特徴とする署名記録の公開方法。

【請求項 10】

請求項 6 記載の署名記録の公開方法であって、  
前記公開機関署名記録公開ステップは、  
前記公開通知書作成ステップに基づいて更新された署名履歴の一部を公開することを特徴とする署名記録の公開方法。

【請求項 11】

請求項 2 記載の署名記録の公開方法であって、  
公開機関署名記録公開通知ステップは、  
通知する前記ユーザを前記ユーザ情報ファイルから検索する送信相手検索ステップと、  
送信すべき履歴を前記ユーザ情報ファイルから検索する送信履歴範囲取得ステップと、  
前記公開機関署名記録を公開したことを通知する公開通知書作成ステップと、  
作成した公開通知書と前回署名の署名記録から署名を作成する署名作成ステップと、  
作成した署名の情報を前記署名履歴に記録する署名履歴更新ステップと、  
通知する前記ユーザの情報を前記ユーザ情報ファイルに記録するユーザ情報ファイル更新ステップと、

10

20

30

40

50

作成した前記公開通知書を前記ユーザに送信する送信ステップと、を有することを特徴とする署名記録の公開方法。

【請求項 1 2】

請求項 1 1 記載の署名記録の公開方法であって、  
前記公開通知書作成ステップは、  
前記公開機関署名記録を公開したことを前記ユーザに伝える文書と、  
公開した署名記録と、  
送信する範囲の署名履歴と、  
に基づいた公開通知書を作成することを特徴とする署名記録の公開方法。

10

【請求項 1 3】

請求項 1 1 記載の署名記録の公開方法であって、  
前記ユーザ情報ファイル更新ステップは、  
前記公開機関署名記録に付けられた署名番号と、  
対応する前記公開機関署名記録が公開機関署名記録公開通知時に作られたことを示す符号と、  
前記公開通知書を送信する前記ユーザを示す相手情報と、  
送信する履歴の範囲を示す情報と、  
とからなる情報を前記ユーザ情報ファイルに追加することを特徴とする署名記録の公開方法。

20

【請求項 1 4】

請求項 1 記載の署名記録の公開方法であって、  
前記ユーザ側装置は、当該ユーザ側装置において送信または受信したユーザ署名記録または公開機関署名記録の、送信または受信相手に関わる情報を記録するユーザ情報ファイルを備えることを特徴とする署名記録の公開方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル署名の証拠性を高める技術に関する。

30

【0002】

【従来の技術】

デジタル署名（以下、署名という）の証拠性を高める技術として、署名作成の際に、その時点までの署名履歴情報を反映させ、作成した署名に関わる情報は、署名記録として新たに署名履歴に追加する手法がある（例えば、特許文献 1 または特許文献 2 参照）。この方法により、作成した署名は連鎖構造を持つ。検証の際は、署名に対する検証の他に、連鎖の検証も行うことにより、改竄は困難となる。

【0003】

この手法においては、連鎖が繋がっている署名は正当なものであると判断するが、その正当性を確実に証明するためには、署名履歴中に信頼できる正当な署名記録があることが望ましい。この信頼できる署名記録を作り出すために、上記手法では、解決策の一つとして、署名記録の定期的な公開が挙げられている。

40

【0004】

上記手法を用いて署名を作成する各ユーザは、定期的もしくは定数回毎に最新の署名記録を公開する。署名記録を例えば、新聞や官報などの刊行物（以下、新聞という）に公開することにより、正当な署名作成者以外が作成した不正な署名記録は、正当な署名作成者の指摘により発覚するため、公開した署名記録は、正当な署名記録であるものとして扱うことができる。また、一般に公開されるため、公開した署名記録は、後から取り消したり、改竄したりすることは困難である。

【0005】

50

## 【特許文献1】

特開2001-331104号公報

## 【特許文献2】

特開2001-331105号公報

## 【0006】

## 【発明が解決しようとする課題】

上記技術において、ユーザの数が多い場合、各ユーザの署名記録を全て新聞に公開することは現実的に難しい。従って、より実用的な仕組みが望まれる。

## 【0007】

## 【課題を解決するための手段】

本発明は、各ユーザが個別に新聞公開するのではなく、その新聞公開をまとめて代行する公開機関を設ける。

## 【0008】

すなわち、本発明は、公開機関側装置およびユーザ側装置のための効率的で安全な公開システムと、ユーザに対して、公開された署名記録を利用した署名検証機能を提供する。

## 【0009】

本発明において、「署名記録」とは、作成あるいは受信した個々の署名の生成に関わる情報であり、「署名履歴」とは、複数の「署名記録」が保存されたファイルを指す。

## 【0010】

本発明の公開システムでは、ユーザ側装置は、署名作成時に他の署名記録から得られる情報を反映させる署名技術（以下、ヒステリシス署名という）を利用し、作成した署名記録を署名履歴に追加する。さらに作成した署名記録を、公開依頼書に添付して公開機関に送信して公開を依頼する。

## 【0011】

公開機関側装置は、各ユーザ側装置から公開依頼書に添付されたユーザ署名記録（以下、公開署名記録という）を受信し、Webなどを利用して第3者がアクセス可能なように公開する。これにより、各ユーザは、各々が署名記録を新聞公開したのと同等の信頼性を得ることができるので、自身の署名履歴中に信頼できるポイントを作ることができる。また、各ユーザは公開された署名記録を任意の時間に任意の場所で取得することができる。取得した署名記録は、正当な署名記録として連鎖検証の起点に利用される。

## 【0012】

また、公開機関側装置は、各ユーザから送られてきた公開署名記録を公開機関が管理するWeb等に公開した際には、それぞれのユーザに対して署名付きのWeb公開通知書を送付する。これによりユーザは、自分の公開署名記録が確実に公開機関によって公開されたことを知ることができる。正規のユーザ側に、公開依頼した覚えが無いのにWeb公開通知書が届いた場合は、他人のなりすましによって不正に公開されたことになる。

## 【0013】

また、公開機関側装置は、公開時にタイムスタンプを取得し、Web公開通知書にこのタイムスタンプを添付してもよい。このタイムスタンプにより、Web公開通知書を受け取ったユーザは、公開日時を確認することができる。また、タイムスタンプの添付されたWeb公開通知書に公開機関の署名が付けられた場合、公開した署名記録の内容と公開日時が保証され、このWeb公開通知書の情報を用いることにより、ユーザの署名履歴中に日時の確定した署名記録を作ることができる。すなわち、その署名記録以前（以後）に作られた署名は、Web公開通知書に記載の日時以前（以後）に作られたものであることを証明することができる。

## 【0014】

公開機関自身も公開機関の署名履歴を持ち、公開機関側装置は、ユーザ側装置から公開署名記録を受信した時、署名の検証を行うとともに、受信した公開署名記録を含んだ公開機関の署名記録を作成し、公開機関の署名履歴を更新する。また、公開機関側装置は、ユーザ側装置へのWeb公開通知書送信の時には、署名の作成を行うとともに、公開機関の署

10

20

30

40

50

名履歴を更新する。公開機関側装置において、各ユーザ側装置から受け取った公開署名記録を含んだ署名記録を公開機関の署名履歴に追加することにより、公開機関あるいはユーザが公開機関の署名履歴の連鎖を調べることによって、公開後の公開署名記録の改竄を検知できるようになる。また、公開機関側装置は、ユーザ側装置から公開署名記録を受信した時や、ユーザへWeb公開通知書を送信した時には、署名履歴の更新とともに公開機関のユーザ情報ファイル（ユーザ情報を保存したファイル）も更新する。ユーザ情報ファイルは、Web公開通知書の送付や署名履歴の送信の際に、送信先や送信する署名履歴の範囲を確定するために参照される。

#### 【0015】

また、公開機関側装置は、公開署名記録を公開機関に送信したユーザに対して、そのユーザから公開署名記録を受信した時点から、その後最初に新聞公開した時点の間に作られた公開機関の署名履歴を送信する。これによりユーザ側装置は、署名検証（連鎖検証を含む）の際に、この送信された署名履歴を利用して、公開機関が新聞に公開した署名記録から公開機関の署名履歴の連鎖をたどって署名検証を行うことができる。

10

#### 【0016】

また、公開機関側装置は、適当な時期に、または定期的に（例えば、毎週1回）、新聞に公開機関の署名履歴中の署名記録を公開する。また、公開機関側装置は、各ユーザ側装置から送られてきた公開署名記録を用いて新聞公開用データを作成し、それを公開してもよい。公開された署名記録あるいは新聞公開用データを用いて署名検証を行うことにより、公開機関の署名履歴の正当性を保証し、公開機関自身の公平性を示すことができる。

20

#### 【0017】

本発明によれば、公開機関がユーザ側装置の署名記録の公開を代行することにより、より多くのユーザが自身の署名の正当性を証明できるようになる。

#### 【0018】

#### 【発明の実施の形態】

図1は、本発明を適用した一実施形態における公開システムの概略図である。

#### 【0019】

図示するように、本公開システムは、署名記録の公開を依頼し、公開機関から受け取った署名履歴を利用して署名を検証するユーザ側装置101～103と、各ユーザから送られてきた署名記録を公開、また自身の署名記録もしくは正当性を示す署名履歴を公開、署名の検証に必要な署名履歴を各ユーザに送信する公開機関側装置104とを含んで構成される。ユーザ側装置101～103と公開機関側装置104は、ネットワーク105を介して繋がっている。

30

#### 【0020】

公開機関側装置104は、図2に示すように、記憶装置202と、ネットワークを介して他の装置と通信を行うための通信装置204と、通信装置204を介して繋がるWebサーバ207と、キーボードやマウスなどの入力装置205と、ディスプレイなどの表示装置206と、CPU201とから構築することができる。

#### 【0021】

記憶装置202には、公開システムの機能を実現するプログラム（公開依頼書受信プログラム208、公開通知書送信プログラム209、新聞公開プログラム210、履歴送信プログラム211、ユーザ管理プログラム212）と、署名履歴ファイル（署名履歴ともいう）213と、ユーザ情報ファイル214と、各ユーザから受信した署名記録等が保存されている公開署名記録保存ファイル215が格納されている。プログラム208～212は、CPU201により実行され、署名の作成や検証、ユーザから受信した署名記録の保存とWeb公開、公開機関自身の署名記録の新聞公開、公開機関の署名履歴の読込や更新、公開機関のユーザ情報ファイルの読込や更新を行う機能を、公開機関側装置上に具現化する。

40

#### 【0022】

各プログラムは、予め記憶装置202に格納されていてもよいし、公開機関側装置が利用

50



可能な媒体を介して導入されてもよい。媒体とは、たとえば、公開機関側装置に着脱可能な記憶媒体や、通信装置204に接続するネットワークまたはネットワークを伝搬する搬送波といった通信媒体を含む。

#### 【0023】

ユーザ側装置は、図3に示すように、記憶装置302と、ネットワークを介して他の装置と通信を行うための通信装置304と、キーボードやマウスなどの入力装置305と、ディスプレイなどの表示装置306と、CPU301とから構成される。

#### 【0024】

記憶装置302には、署名を作成して署名付き文書を送信する送信プログラム307と署名付き文書を受信して署名を検証する受信プログラム308と署名履歴の連鎖検証も含んだ検証を行う文書検証プログラム309と公開依頼書を作成して公開書名記録を公開機関に送信する公開依頼書送信プログラム310と自分の署名履歴を他のユーザに送信する履歴送信プログラム311と他のユーザから他のユーザの署名履歴を受信する履歴受信プログラム312と署名履歴ファイル（署名履歴という）313とユーザ情報ファイル314と他ユーザから受信した署名履歴を保存するファイル315が格納されている。プログラム307～312は、CPU301により実行され、署名の作成や検証、署名履歴の読込や更新、ユーザ情報ファイルの読込や更新を行う機能を、ユーザ側装置101～103上に具現化する。

#### 【0025】

ユーザ側装置101～103は、署名作成時に署名履歴情報を反映させるヒステリシス署名技術を利用している。

#### 【0026】

図4は、ユーザ側装置101～103が、ヒステリシス署名技術に基いて、送信文書407に対し署名を作成した後、署名付き受信文書409を受信し署名検証した場合の署名履歴の様子を示したものである。

#### 【0027】

署名作成時には、送信文書407と前回の署名記録413のハッシュ値に対して秘密鍵を作用させて署名408を作成する。作成後、前回の署名記録413と作成した署名408から、署名記録414を作成し、署名履歴313に追加する。どの署名がどの署名記録中に残っているか判別するために、署名作成時においては、署名履歴に今回新たに追加される署名記録の署名番号を、作成した署名に付加する。作成された署名記録が順に記録されたファイルが署名履歴313である。

#### 【0028】

署名受信時には、受信文書409に対する署名410を公開鍵を用いて検証する。検証後、前回の署名記録414のハッシュ値と署名410から署名記録415を作成し、署名履歴411に追加する。以上のように、署名作成時や署名受信時において、署名情報を記録した署名記録が作られる。前回の署名情報が次の署名作成に利用されるため、署名間に連鎖関係が生じる。通常の公開鍵を用いた署名検証に加えて、この連鎖関係を検証することにより、より確実な署名の検証を行うことができる。

#### 【0029】

ユーザ側装置101～103における署名記録412～415は、署名アルゴリズム等の情報を示す「識別番号401」、何番目に作られた署名記録であることを示す「署名番号402」、署名作成（送信）時に作成した署名記録か、署名検証（受信）時に作成した署名記録かを表す「種別403」、連鎖検証に利用する「前回署名記録のハッシュ値404」、署名作成時のみ記録する「署名作成対象文書のハッシュ値（文書のハッシュ値という）405」、「署名or受信署名記録情報406」（署名作成時は、作成した署名。署名検証時は、受信した署名の署名番号とその署名に対する署名記録のハッシュ値を結合したもの）から成る。

#### 【0030】

図5にユーザと公開機関の間でやり取りされるデータの流れを図示する。

## 【0031】

ユーザ側装置101～103は、適当な時期あるいは定期的に、公開したい署名記録（たとえばその時点での最新の署名記録）を添付した公開依頼書506を公開機関側装置104に送信する（501）。これにより、ユーザの署名履歴313中に信頼性を保証された署名記録を作ることが可能となる。この公開機関に送信した署名記録は、公開署名記録という。

## 【0032】

ユーザ側装置101～103より公開署名記録を受け取った公開機関側装置は、その公開署名記録を自身の記憶装置202に保管するとともに、Webなどを利用して公開する（502）。公開後に、公開した公開署名記録の作成者であるユーザに対して、公開した旨を知らせるWeb公開通知書507を送信する（503）。 10

## 【0033】

公開機関は、適当な時期、あるいは定期的に新聞に自身の署名記録を公開（公開した署名記録を以降、新聞公開署名記録と呼ぶ）する（504）。新聞公開後に、前回の新聞公開時点から今回の新聞公開時点までの間に、ステップ502で公開された公開署名記録の公開を依頼したユーザに対して、新聞公開した旨を知らせる新聞公開通知書508を送信する（505）。新聞公開通知書には、ユーザが新聞公開署名記録を利用して署名の検証が行えるような情報を添付する。

## 【0034】

本実施例においては、公開機関側装置104も、署名作成時に署名履歴情報を反映させる上記ヒステリシス署名技術を利用する。図6は、公開システムの機能を実現するための、公開機関側装置104の署名履歴213とユーザ情報ファイル214の構成の一例である。 20

## 【0035】

公開機関側装置104の署名履歴ファイル213は、公開機関側装置で作成された署名記録が順に記録されたファイルであり、各レコード601～603は、識別番号604、署名番号605、種別606、前回署名記録のハッシュ値607、公開機関側装置で作成する署名の対象となる文書のハッシュ値（文書のハッシュ値という）608、署名or受信した公開署名記録情報609（署名作成時は、作成した署名。署名検証時は、受信した公開署名記録の署名番号と公開署名記録のハッシュ値を結合したもの）からなる。 30

## 【0036】

「識別番号604」は、公開機関側装置104が利用している署名アルゴリズム等の情報を示す番号であり、これによって、署名記録601～603が作成された時に、どの種類の暗号やハッシュ関数が使われたのかを判別する。

## 【0037】

「署名番号605」は、連番で付与され、署名履歴の中から特定のレコード（署名記録）を指定するのに用いられる。どの署名がどの署名記録中に残っているか判別するために、署名作成時には、署名履歴に今回新たに追加される署名記録の「署名番号605」を、作成した署名に付加する。

## 【0038】

「種別606」は、署名記録601～603が署名作成（送信）時に作成されたものか、署名検証（受信）時に作成されたものかを示す符号であり、例えば、署名記録601は、種別606の値により、署名検証（受信）時に作成されたものであると分かる。 40

## 【0039】

「前回署名記録のハッシュ値607」は、署名履歴の連鎖検証に用いられるものであり、例えば、署名番号「2」で指定される署名記録602における「前回署名記録のハッシュ値607」の「H(S1)」は、署名記録601における各項目604～609の各値からなるデータS1（S1はたとえば各値を結合する）のハッシュ値（ハッシュ関数をH(x)とする）である。

## 【0040】

「文書のハッシュ値608」を署名履歴213の項目のひとつに含めてもよい。この項目を用いることによって、改竄するためには、それに対応する署名の作成対象となった文書が必要となるため、改竄がより困難になる。

【0041】

「署名or受信した公開署名記録情報609」には、公開機関装置での署名作成（送信）時には、作成した署名を登録する。例えば、署名記録602においては、署名番号「2」、前回署名記録のハッシュ値「H(S1)」、文書のハッシュ値608「H(M2)」からなるデータに対する署名「Sign(2||H(S1)||H(M2))」を登録する。また、公開依頼書506を受信した時には、添付されていた公開署名記録の署名番号とハッシュ値とからなるデータを登録する。例えば、署名記録603においては、「署名or受信した公開署名記録情報609」には、受信した公開依頼書506に添付された公開署名記録の署名番号が「15」で、公開署名記録のハッシュ値が「H(S15)」であれば、これらを結合した「15||H(S15)」を登録する。

10

【0042】

ユーザ情報ファイル214は、公開機関側装置での取引記録が順に記録されたファイルであり、各レコード610～616は、署名番号617、種別618、取引相手の情報（相手情報という）619、受信した署名の署名番号（受信署名番号という）620、公開署名記録621、タイムスタンプの日時（日時という）622からなる。

【0043】

「署名番号617」には、何番の署名記録が誰と署名を取引した時に作成されたものであるかが分かるように、署名記録の署名番号605と対応した番号が登録する。

20

【0044】

「種別618」は、610～616の各レコード（取引記録）が署名作成（送信）時に作成されたものであるか、署名検証（受信）時に作成されたものであるか、新聞公開時504に作成されたものであるか、新聞公開通知書送信（署名履歴送信）時505に作成されたものであるかを示す符号である。例えば、署名番号「3」で指定されるレコード613は、項目618の値により、署名検証（受信）時に作成されたものであると分かる。

【0045】

「相手情報619」には、署名付き文書の送信相手や公開依頼書506の送信元などの情報（例えば、メールアドレス）を登録する。例えば、署名番号「3」で指定されるレコード613は、項目619の値により、ユーザBとの取引情報を示すものであることが分かる。

30

【0046】

「受信した署名の署名番号（受信署名番号という）620」には、受信した公開依頼書などの署名付き文書に付けられていた署名の署名番号を登録する。例えば、署名番号「3」で指定されるレコード613は、項目620の値により、「16」の署名番号の署名が付いた署名付き文書を受信した時に作成されたものである。

【0047】

「公開署名記録621」には、公開署名記録が添付された公開依頼書506を受信した時に、その添付されていた公開署名記録を登録する。例えば、署名番号「3」で指定されるレコード613は、項目621の値により、公開署名記録「S15」が添付された公開依頼書を受信した時に作成されたものである。

40

【0048】

「日時622」には、公開依頼書に添付された公開署名記録を受信した（502）時の日時、あるいは、公開機関の署名記録を新聞公開した（504）時の日付を登録する。

【0049】

「署名番号617」により、例えば、署名履歴213の署名番号「3」で指定されるレコード603とユーザ情報ファイル214の署名番号「3」で指定されるレコード613とは対応していることが分かり、署名記録603は、取引記録613の各値により、ユーザBから公開依頼書を受信した時に作成されたものであり、公開依頼書には、署名番号「1

50

6」の署名と、公開署名記録「S 1 5」が添付されており、この公開署名記録「S 1 5」は、「2002年10月19日15時50分」に公開機関側装置が受信したものであると分かる。

【0050】

ユーザ側装置101～103も、ユーザ情報ファイル314を持つ。ユーザ情報ファイル314は、他のユーザとの取引情報、公開機関との取引情報を調べるのに利用される。ユーザ側装置のユーザ情報ファイル314は公開機関側装置のユーザ情報ファイル214とは異なり、ユーザ側装置のユーザ情報ファイルには項目620「公開署名記録」、項目621「日時」に該当する部分はない。ユーザ側装置のユーザ情報ファイル314は、何番の署名記録は誰と取引した署名のものであるかが分かるように、署名記録の署名番号と対応する「署名番号」、対応する署名記録が、署名作成（送信）時に作られたか、署名検証（受信）時に作られたか、公開機関に公開した時に作られたかを表す「種別」、「取引相手の情報（相手情報という）」、「受信した署名の署名番号（受信署名番号という）」で構成する。

10

【0051】

公開機関側装置は、公開システムの公開依頼書受信プログラム208を用いて、ユーザから送信されてきた公開署名記録が添付された署名付き公開依頼書506を受信する。

【0052】

図7にユーザによる公開依頼書送信プログラム310と公開機関の公開依頼書受信プログラム208のフロー図を示す。

20

【0053】

ユーザ側装置101～103において、S701で、公開したい情報（公開署名記録）を取得し、それを添付した公開依頼書506を作成する。S702で、S701で作成した公開依頼書に対して署名を作成し、S703で署名付き公開依頼書を公開機関側装置に送信する。

【0054】

公開依頼書を受信した公開機関側装置において、S704で、まずユーザが公開機関に登録されているか、すなわちユーザが正規の公開機関利用者であるかどうかを、例えば登録データベース（公開機関を利用希望するユーザを登録したリスト）を用いて確認し、公開依頼書に署名が付けられている場合は、S705で、送信元ユーザの公開鍵を用いて署名を検証する。公開鍵は、公開鍵証明書とともに署名付き公開依頼書に添付されていればその公開鍵を利用し、あるいは公開鍵証明書発行元より取得すればよい。

30

【0055】

署名検証後、S706で、受信したユーザの公開署名記録を用いて、「識別番号604」、「署名番号605」、「前回署名記録のハッシュ値607」、「受信した公開署名記録情報609」を、たとえば結合して作成した署名記録を作成し、署名履歴213に追加する。

【0056】

S707で、タイムスタンプを取得し、S708で、ユーザ情報ファイルに、S706で作成した署名記録の「署名番号617」、公開依頼書を受信したことを示す「受信符号618」、公開依頼書を送信した送信元のユーザ情報である「相手情報619」、「受信した署名の署名番号（公開依頼書にS702によって署名が付けられていた場合）620」、受信した「公開署名記録620」、取得したタイムスタンプを用いた「日時621」を記録する。タイムスタンプは、例えばタイムスタンプ発行機関から取得すればよい。また、上記送信元のユーザ情報としては、例えばメールアドレスを登録すればよい。

40

【0057】

図7のS703において、ユーザAから署名番号31の公開署名記録S31が添付された公開依頼書が公開機関に送信された場合には、S706によって、署名履歴213の各項目604～609の値「Ver. 1. 0（公開機関が利用する署名アルゴリズム等の情報を示す値）」、「1」、「受信」、「H(S0)（前回の署名記録のハッシュ値）」、「

50

ー（受信時なので、文書のハッシュ値は無し）」、「31 || H (S31)」が結合したレコード601が新たに記録される。

【0058】

S708によって、ユーザ情報ファイル214の各項目617～622の値「1」、「受信」、「ユーザA@XXX.co.jp（ユーザAのメールアドレス）」、「32（S702によって公開依頼書に付けられた署名の署名番号）」、「S31」、「2002.10.17.0816（公開依頼書を受信した日時）」が結合したレコード611が新たに記録される。

【0059】

S709で、Web上に公開依頼書送信元のユーザ名と公開依頼書に添付された公開署名記録を公開する。

10

【0060】

公開機関側装置104は、公開依頼書受信プログラム208により、ユーザから受信した公開署名記録をWebに公開（502）した後、Web公開通知書送信プログラム209により、その公開署名記録の送信元のユーザにWebに公開した旨を伝えるWeb公開通知書507を送信する。

【0061】

公開機関側装置104の公開通知書送信プログラム209の処理フローについて、図8を用いて説明する。

【0062】

20

S801で、公開依頼書を送信してきたユーザに対してWebに公開した旨を伝えるWeb公開通知書507を作成する。Web公開通知書には、上記公開依頼書を送信してきたユーザから依頼されて公開した公開署名記録（公開依頼書に添付されていた署名記録）やS707により取得したタイムスタンプなどを添付しても良い。添付した場合には、公開機関がそのWeb公開通知書に署名をつけると、Web公開通知書を受け取ったユーザは公開署名記録がいつ公開されたかを証明することができ、少なくともその日時以前にその署名記録が存在していたことを示すことができる。

【0063】

S802で、新たな署名番号（前回作成した署名記録の署名番号に1足したもの）と前回署名記録のハッシュ値とS801で作成したWeb公開通知書のハッシュ値からなるデータをたとえば結合により作成して、それに対して署名を作成する。例えば、署名履歴213にレコード601が記録された状態で、公開通知書送信プログラム209によりユーザAにWeb公開通知書を送信する時には、署名番号605の「1」に1を足した値「2」と前回署名記録601のハッシュ値607「H(S1)」と文書のハッシュ値（ここではWeb公開通知書のハッシュ値）608「H(M2)」から、署名「Sign(2 || H(S1) || H(M2))」を作成する。

30

【0064】

S803で、S802で作成した署名に関する情報を署名記録として、署名履歴213に追加する。この時の署名記録は、上記例の場合は、識別番号604「Ver. 1.0（公開機関が利用する署名アルゴリズム等の情報を示す値）」、署名番号605「2」、種別606「送信」、前回署名記録のハッシュ値607「H(S1)」、文書のハッシュ値608「H(M2)（Web公開通知書のハッシュ値）」、署名609「Sign(2 || H(S1) || H(M2))」から、たとえば結合により作成する。作成したレコード602が署名履歴213に新たに記録される。

40

【0065】

S804で、ユーザ情報ファイル214に、「署名番号617」、「種別618」、「相手情報619」を記録する。上記例の場合は、各々、S803で作成した署名記録の署名番号「2」、Web公開通知書を送信したことを示す送信符号「送信」、Web公開通知書の送信先のユーザ情報（例えば、メールアドレス）「ユーザA@XXX.co.jp（Web公開通知書の送信先のユーザAのメールアドレス）」が結合されたレコード612

50

がユーザ情報ファイル 2 1 4 に新たに記録される。

【 0 0 6 6 】

S 8 0 5 で、S 8 0 2 で作成した署名の付いた W e b 公開通知書をユーザに送信する。

【 0 0 6 7 】

図 5 に示すように、公開機関は、適当な時期に、または定期的に公開機関の署名履歴中の最新の署名記録を新聞などに公開する ( 5 0 4 ) 。これによって、公開機関の署名履歴中に、公開後は変更不可能な署名記録、すなわち信頼できる署名記録を作り出すことができる。公開機関の署名履歴中に信頼できる署名記録を作り出すことによって、公開機関自体の不正を防ぎ、ユーザから、より大きな信用を得る。

【 0 0 6 8 】

新聞公開した信頼できる署名記録から連鎖が辿れる署名履歴は正当なものであり、ユーザは、新聞等に公開した公開機関の署名記録、公開機関の署名履歴、各ユーザの公開署名記録、各ユーザの署名履歴を用いて、署名を検証することができる。

【 0 0 6 9 】

公開機関側装置 1 0 4 の新聞公開プログラム 2 1 0 の処理フローを図 9 を用いて説明する。

【 0 0 7 0 】

S 9 0 1 で、新聞公開するデータを取得する。具体的には、署名履歴 2 1 3 中、最新の署名記録を取得する。例えば、署名履歴 2 1 3 にレコード 6 0 1 ~ 6 0 3 が記録されている状態であるとする、署名記録 6 0 3 が新聞公開の対象となる ( 新聞公開署名記録と呼ぶ ) 。

【 0 0 7 1 】

S 9 0 2 で、今回作成する署名の署名番号 ( 前回作成した署名記録の署名番号に 1 足したもの ) と前回署名記録のハッシュ値と新聞公開署名記録のハッシュ値とからなるデータをたとえば結合により作成し、それに対して署名を作成する。

【 0 0 7 2 】

S 9 0 3 で、S 9 0 2 で作成した署名に関する情報を署名記録として、署名履歴 2 1 3 に追加する。署名記録は、「識別番号 6 0 4 」、「署名番号 6 0 5 ( 今回作成した署名の署名番号 ) 」、「前回署名記録のハッシュ値 6 0 7 」、「文書のハッシュ値 6 0 8 ( 新聞公開署名記録のハッシュ値 ) 」、「署名 6 0 9 ( S 9 0 2 で作成した署名 ) 」を結合したものである。

【 0 0 7 3 】

S 9 0 4 で、S 9 0 3 で作成した署名記録の「署名番号 6 1 7 」、「種別 6 1 8 」、「相手情報 6 1 9 」、「公開署名記録 6 2 1 」、「日時 6 2 2 」をユーザ情報ファイル 2 1 4 に記録する。上記例の場合は、例えば、各々、「新聞公開したことを示す新聞公開符号」「公開先の情報 ( 公開先名 ) 」「新聞公開署名記録」「公開日時」がレコード 6 1 5 に記録される。

【 0 0 7 4 】

S 9 0 5 で、新聞公開署名記録を新聞に公開する。このとき、公開機関の署名をつけて公開しても良いし、新聞公開署名記録のハッシュ値を公開しても良い。

【 0 0 7 5 】

公開機関は、新聞公開を行った後、前回の新聞公開から今回の新聞公開までの期間で受信した公開署名記録について、その送信元のユーザに、履歴送信プログラム 2 1 1 を用いて、公開機関の署名履歴を送信する。これにより、公開機関だけではなく各ユーザの手元にも、公開機関の新聞公開署名記録からユーザの署名履歴まで連鎖を遡って検証できる情報を残すことができる。例えば、10 年後に万一、公開機関が無くなってしまっても、各ユーザの手で検証が可能となる。

【 0 0 7 6 】

履歴送信プログラム 2 1 1 の処理フローについて図 6 と図 1 0 を用いて説明する。

【 0 0 7 7 】

10

20

30

40

50

S 1 0 0 1では、署名履歴を送信する相手を公開機関のユーザ情報ファイル2 1 4から検索する。検索の際には、最新の新聞公開署名記録を新聞公開した時点から、前回新聞公開署名記録を新聞公開した時点までの間で、公開機関がWeb公開通知書を送信した送信先のユーザを特定する。具体的には、種別6 1 8に新聞公開したことを示す符号が付いている最新の取引記録(レコード)とそれ以前で最新の新聞公開符号が付いている取引記録との間の取引記録を調べ、種別6 1 8に送信符号が付いている取引記録を探す。その取引記録の相手情報6 1 9が、署名履歴を送信する相手に関する情報である。

#### 【0 0 7 8】

例えば、ユーザ情報ファイル2 1 4において、種別6 1 8を見てみると、「新聞」により、レコード6 1 5が最新の新聞公開した時の取引記録であり、レコード6 1 0が前回新聞公開した時の取引記録であることが分かる。それらの間のレコード6 1 1～6 1 4の種別6 1 8に「送信」が登録されているレコードは、6 1 2と6 1 4である。レコード6 1 2と6 1 4の相手情報6 1 9により、署名履歴を送信すべき相手は、ユーザAとユーザBであることが分かる。

#### 【0 0 7 9】

S 1 0 0 2で、ユーザ情報ファイル2 1 4を利用して、S 1 0 0 1で特定した送信先に、どの範囲の署名履歴を送信すればよいか求める。まず(1) S 1 0 0 1で特定した署名履歴送信先が記録されていた取引記録の署名番号を調べ、(2)次に最新の新聞公開した署名記録の署名番号を調べる。(1)の署名番号から(2)の署名番号までが送信する履歴の範囲である。例えば、S 1 0 0 1において、レコード6 1 2によりユーザAが署名履歴の送信先として特定されたとすると、レコード6 1 2の項目6 1 7の値が1であり、レコード6 1 5の署名番号6 1 7の値が5であるから、署名番号6 1 7の値が1～5の署名履歴が、ユーザAに送信すべき履歴の範囲である。

#### 【0 0 8 0】

S 1 0 0 3では、S 1 0 0 2で決定した範囲の署名履歴を添付した新聞公開通知書5 0 8を作成し、

S 1 0 0 4で、今回作成する署名の署名番号(前回作成した署名記録の署名番号に1足したもの)と前回署名記録のハッシュ値と新聞公開通知書のハッシュ値とからなるデータに対して署名を作成する。

#### 【0 0 8 1】

S 1 0 0 5で、S 1 0 0 4で作成した署名に関する情報を署名記録として、署名履歴2 1 3に追加する。署名記録は、識別番号6 0 4、署名番号6 0 5、前回署名記録のハッシュ値6 0 7、文書のハッシュ値(ここでは、新聞公開通知書のハッシュ値)6 0 8、署名6 0 9(S 1 0 0 3で作成した署名)を結合したものである。

#### 【0 0 8 2】

S 1 0 0 6で、ユーザ情報ファイル2 1 4の、例えばレコード6 1 6のように、署名番号6 1 7、種別6 1 8、相手情報6 1 9にそれぞれ、S 1 0 0 5で作成した署名記録の署名番号、新聞公開通知書を送信したことを示す履歴送信符号、新聞公開通知書の送信先のユーザ情報(例えば、メールアドレス)を記録する。

#### 【0 0 8 3】

S 1 0 0 7で、S 1 0 0 4で作成した署名付き新聞公開通知書をユーザに送信する。

#### 【0 0 8 4】

公開機関側装置1 0 4では、公開機関を利用するユーザおよび、ユーザから受信した公開署名記録をユーザ管理プログラム2 1 2によって管理する。公開機関側装置ではユーザ管理プログラム2 1 2を用いて、自身のデータベースに公開機関を利用するユーザを登録する。また、ユーザの要望、もしくは公開機関の判断で、ユーザ情報の追加・更新、ユーザの削除を行ってもよい。

#### 【0 0 8 5】

ユーザが公開機関に公開署名記録の公開を依頼し、公開機関側装置が公開依頼書受信プログラム2 0 8によってユーザの公開署名記録を公開し、新聞公開プログラム2 1 0によ

10

20

30

40

50

て署名履歴 2 1 3 中の署名記録を新聞公開することにより、ユーザは、自分の署名履歴中に新聞公開したのと同等の信頼性を持つ署名記録を持つことができる。

【 0 0 8 6 】

図 1 1 を用いて、検証に利用できるユーザの署名履歴や公開機関の署名履歴を持つユーザ側装置の文書検証プログラム 3 0 9 が検証対象文書の署名を検証する場合を例にあげて説明する。

【 0 0 8 7 】

図 1 1 において、ユーザが署名番号 2 の署名が添付された文書 1 2 1 0 を検証する場合、S 1 2 0 1 で、文書と署名に対して公開鍵を用いた通常の署名検証を行い、S 1 2 0 2 で、検証に利用するユーザ側装置の署名履歴 3 1 3 中の署名番号 2 の署名記録の項目 6 0 9 に、検証対象の N o . 2 の署名が残っているかどうか検証する。

【 0 0 8 8 】

S 1 2 0 3 で、署名履歴 3 1 3 中 N o . 2 以降で N o . 2 に一番近い公開署名記録を検索する（本例では、N o . 7 がそれに該当する署名記録とする）。公開依頼書に添付する公開署名記録は、それまでの最新の署名記録であるので、N o . 8 の署名記録が公開機関に公開依頼書を送信した時に作成されたとすると、この時公開された公開署名記録は、N o . 7 の署名記録であることが、ユーザ情報ファイル 3 1 4 よりわかる。従って、N o . 2 以降で N o . 2 に一番近い公開署名記録は、N o . 7 の署名記録である。ただし、N o . 2 以降であれば、必ずしも一番近い公開署名記録でなくてもよい。

【 0 0 8 9 】

S 1 2 0 4 で、検証に必要なデータを取得する。ここで検証に必要なデータとは、N o . 2 の署名の情報が残っている署名履歴 3 1 3 と、新聞公開署名記録 1 2 1 4 （公開機関の N o . 1 0 5 の署名記録）と、公開機関の N o . 1 0 5 の署名記録が新聞公開された時に、ユーザによる N o . 7 の公開署名記録の公開依頼に対して、公開機関側装置から送信された公開機関の N o . 1 0 1 ~ N o . 1 0 5 の署名履歴 2 1 3 である。新聞公開署名記録は、検証に利用する署名履歴 2 1 3 中に含まれていなければならない。検証に利用する新聞公開署名記録が公開機関側装置から送られた署名履歴に含まれていない場合は、必要な公開機関の署名履歴 2 1 3 を、検証するユーザが要請して取得しても良い。

【 0 0 9 0 】

S 1 2 0 5 で、連鎖の検証を行う。連鎖の検証は、以下のステップにより行う。

【 0 0 9 1 】

S 1 2 0 6 で、新聞公開署名記録（N o . 1 0 5）1 2 1 4 が、公開機関の署名履歴 2 1 3 中の N o . 1 0 5 の署名記録と一致するかどうか検証する。

【 0 0 9 2 】

S 1 2 0 7 で、新聞公開された公開機関の N o . 1 0 5 の署名記録から、ユーザの N o . 7 の公開署名記録を受信した時に作成した公開機関の署名記録（N o . 1 0 1 の署名記録）まで連鎖が繋がっているか検証する。連鎖検証の際には、署名記録中に残された前回署名記録のハッシュ値 6 0 7 と、その 1 つ前の署名記録のハッシュ値とを比較し、一致すれば前後の連鎖は繋がっており、一致しなければ連鎖は途切れていると判断する。

【 0 0 9 3 】

S 1 2 0 8 で、ユーザの公開署名記録（N o . 7 の署名記録）が添付された公開依頼書を受信した時に作成された公開機関側装置の署名履歴 2 1 3 中の N o . 1 0 1 の署名記録に含まれる「受信した公開署名記録情報 6 0 9」の内容「署名番号と公開署名記録（N o . 7 の署名記録）のハッシュ値を結合したもの」と、ユーザ側装置の署名履歴 3 1 3 中の N o . 7 の署名記録に含まれる項目 6 0 9 の内容「署名番号と N o . 7 の署名記録のハッシュ値を結合したもの」が一致するか検証する。

【 0 0 9 4 】

S 1 2 0 9 で、ユーザ側装置の署名履歴 3 1 3 において、公開署名記録（N o . 7 の署名記録）から検証対象署名の署名記録（N o . 2 の署名記録）までの連鎖を検証する。連鎖検証の際には、署名記録中に残された「前回署名記録のハッシュ値 4 0 4」と、その 1 つ

10

20

30

40

50



前の署名記録のハッシュ値とを比較し、一致すれば前後の連鎖は繋がっており、一致しなければ連鎖は途切れていると判断する。

【0095】

以上、S1206からS1209まで全ての検証が成功すれば、連鎖の検証は成功であり、S1201、S1202、S1205の検証が全て成功すれば、検証対象署名の検証は成功である。

【0096】

上記では、公開機関側装置の署名記録を新聞公開することによって、公開機関の不正を防ぎ、確実に署名の正当性を検証する例を示した。公開機関の署名履歴を使わず、以下に示すような別の方法を用いても良い。

10

【0097】

公開機関側装置は、ある一定の期間に複数のユーザ側装置から受信した公開署名記録を結合し、そのハッシュ値をとる。このハッシュ値を公開用データとして新聞などのメディアを利用して公開することによって、公開機関の不正防止と、各ユーザが公開を依頼した公開署名記録の完全性が保証される。例えば、この公開データが公開された時に、別の検査機関が、公開機関によってWebなどに公開されているユーザの公開署名記録を利用して、公開データが正しいかどうか検証することによって、その署名の正当性を証明することもできる。

【0098】

具体的な手順は以下の通りである。図12において、公開機関側装置104の記憶装置202にはユーザA～Eのユーザ側装置から送られてきた公開署名記録を保存する。受信した公開署名記録は、Webなどに公開する。Webに公開した時に、公開機関がWeb公開通知書507をユーザに送ると、ユーザはWeb公開されたことを確認することができる。公開機関は、記憶装置202に保存された公開署名記録を利用して、定期的に新聞公開504を行う。日時tにおいて、まずその時点で各ユーザが公開機関に公開している最新の公開署名記録1301～1305からなるデータを、たとえば結合により作成する。この作成したデータにハッシュ関数を適用してハッシュ値を求め、そのハッシュ値を新聞公開用データとして新聞に公開する。

20

【0099】

一定時間経過後の日時t+1に同様に、公開署名記録1306～1310に基づくハッシュ値を求め、日時t+1での新聞公開用データとして新聞に公開する。

30

【0100】

上記のような公開データの作成と公開を、適当な時期に、または定期的に行い、新聞公開用データの作成に利用した公開署名記録を作成したユーザ側装置に、新聞公開通知書508を送信する。

【0101】

各ユーザ側装置は、公開された新聞公開用データと、Webなどに公開されている公開署名記録とを比較することによって、公開署名記録の改竄の有無を調べることができる。公開されている各ユーザの公開署名記録が一つでも改竄されていれば、新聞公開用データと、Webに公開されている公開署名記録に基づくハッシュ値とが一致しなくなり、改竄が発覚する。

40

【0102】

上述した公開機関の不正の有無は、各ユーザ側装置ではなく、上述していない他の検査機関の装置において検査してもよい。

【0103】

公開機関側装置104がある一定の期間内に受信した公開署名記録からなるデータに基づいて作成され、公開された新聞公開用データと、ユーザの公開署名記録と署名履歴を用いて、当該ユーザの署名を検証する方法を以下に示す。検証前に、予め、検査機関の報告などを調べて、公開機関によるWeb公開に不正が無いかどうか確認しておく。

【0104】

50

例えば、図 13 において、N o. 2 の署名付き文書 1405 を検証する時、S 1401 で、検証対象文書と検証対象署名に対して公開鍵を用いて通常の署名検証を行い、S 1402 で、検証対象署名と署名履歴 313 の N o. 2 の署名記録の中に検証対象署名があるかどうか検証する。

【0105】

S 1403 で、W e b 公開されている公開署名記録と署名履歴 313 とに含まれる同じ署名番号の署名記録（本例では、N o. 7 の署名記録）が一致するか検証する。

【0106】

S 1404 で、ユーザの署名履歴 313 について、S 1403 で検証した公開署名記録（W e b 公開された公開署名記録と同じ番号の署名記録）から検証対象署名の N o. 2 の署名記録まで連鎖が繋がっているか検証する。連鎖の検証は上記実施例と同様に行う。

【0107】

S 1401 ～ S 1404 の検証が全て成功すれば、検証対象署名の検証は成功である。

【0108】

【発明の効果】

本発明による、公開機関がユーザ側装置の署名記録の公開を代行する仕組みにより、より多くのユーザが自身の署名の正当性を証明できるようになる。

【図面の簡単な説明】

【図 1】本発明の第 1 実施形態が適用されたシステムの概略図である。

【図 2】本公開システムにおける公開機関装置の構成図である。

【図 3】本公開システムにおけるユーザ側装置の構成図である。

【図 4】ヒステリシス署名技術の概略図である。

【図 5】ユーザと公開機関の間でやり取りされる情報を表した図である。

【図 6】署名履歴ファイルに格納されるデータの構成、また、ユーザ情報ファイルに格納されるデータの構成を説明するための図である。

【図 7】公開システムの受信プログラムの処理内容を説明するためのフロー図である。

【図 8】公開システムの送信プログラムの処理内容を説明するためのフロー図である。

【図 9】公開システムの新聞公開プログラムの処理内容を説明するためのフロー図である。

【図 10】公開システムの履歴送信プログラムの処理内容を説明するためのフロー図である。

【図 11】ユーザが、新聞等に公開された公開機関の署名記録、署名履歴送信プログラムによって公開機関より送られてきた公開機関の署名履歴、各ユーザの公開署名記録、各ユーザの署名履歴を用いて、署名を検証する方法を説明した図である。

【図 12】各ユーザから受信した情報を用いて公開用データを作成し、新聞公開する方法を説明した図である。

【図 13】公開機関が、ある一定の期間内に受信した全ての公開署名記録を結合し、そのハッシュ値を公開用データとして新聞公開した場合の、ユーザが、各ユーザの公開署名記録、各ユーザの署名履歴を用いて、署名を検証する方法を説明した図である。

【符号の説明】

101～103：ユーザ側装置、104：公開機関側装置、105：ネットワーク、201：CPU、202：記憶装置、203：インタフェース、204：通信装置、205：入力装置、206：表示装置、207：W e b サーバ、208：公開依頼書受信プログラム、209：公開通知書送信プログラム、210：新聞公開プログラム、211：履歴送信プログラム、212：ユーザ管理プログラム、213：署名履歴ファイル、214：ユーザ情報ファイル、215：公開署名記録保存ファイル、301：CPU、302：記憶装置、303：インタフェース、304：通信装置、305：入力装置、306：表示装置、307：送信プログラム、308：受信プログラム、309：文書検証プログラム、310：公開依頼書送信プログラム、311：履歴送信プログラム、312：履歴受信プログラム、313：署名履歴ファイル、314：ユーザ情報ファイル、315：他ユーザ

10

20

30

40

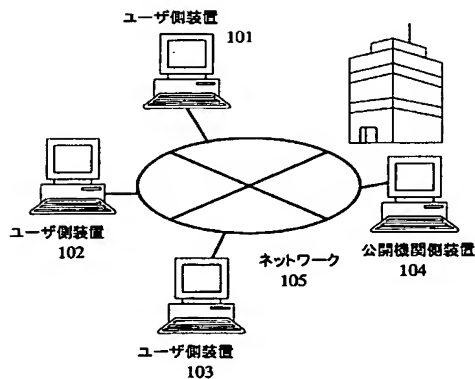
50

署名履歴保存ファイル、401：項目（「識別番号」）、402：項目（「署名番号」）、403：項目（「種別」）、404：項目（「前回署名記録のハッシュ値」）、405：項目（「文書のハッシュ値」）、406：項目（「署名または受信署名記録情報」）、407：送信文書、408、410：署名、409：受信文書、412～415：署名記録、506：公開依頼書、507：Web公開通知書、508：新聞公開通知書、601～603：レコード、604：項目（「識別番号」）、605：項目（「署名番号」）、606：項目（「種別」）、607：項目（「前回署名記録のハッシュ値」）、608：項目（「文書のハッシュ値」）、609：項目（「署名または受信した公開署名記録情報」）、610～616：レコード、617：項目（「署名番号」）、618：項目（「種別」）、619：項目（「相手情報」）、620：項目（「受信署名番号」）、621：項目（「公開署名記録」）、622：項目（「日時」）、1210：検証対象文書、1214：新聞公開署名記録、1301～1305：日時 $t$ で各ユーザが公開機関に公開している最新の公開署名記録、1306～1310：日時 $t+1$ で各ユーザが公開機関に公開している最新の公開署名記録、1405：検証対象文書、1406：ユーザの署名履歴。

10

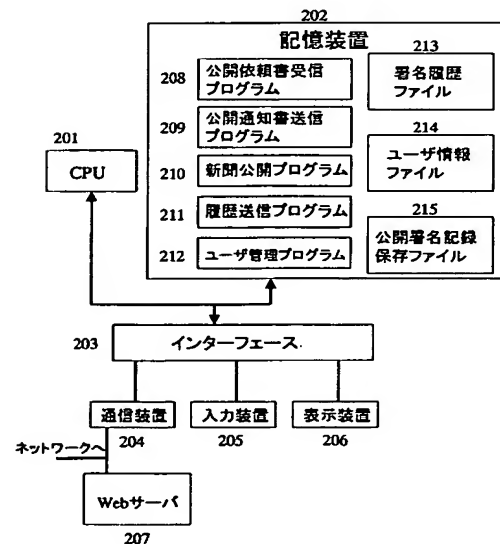
【図1】

図1



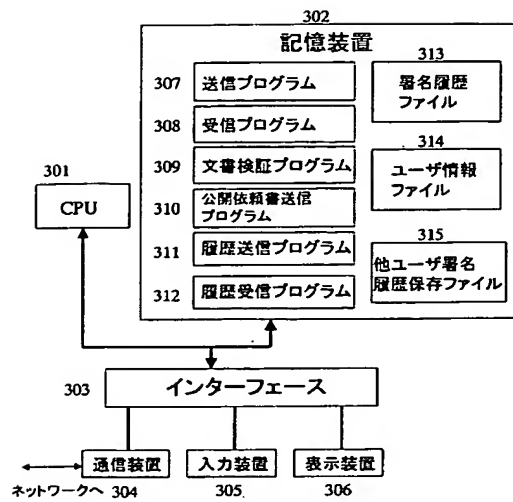
【図2】

図2



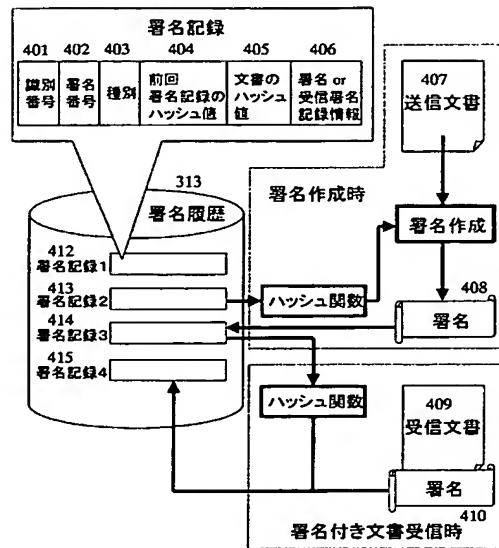
【図3】

図3



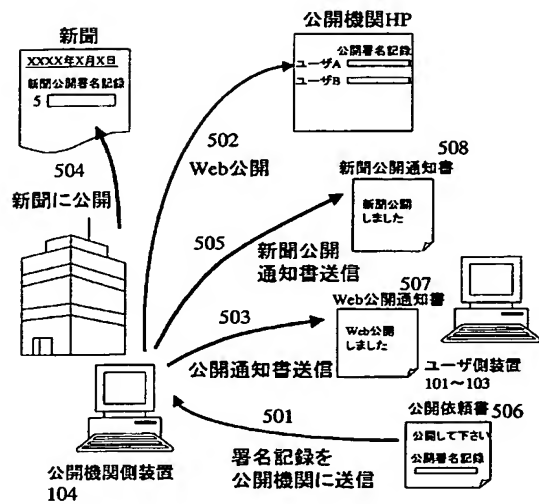
【図4】

図4



【図5】

図5



【図6】

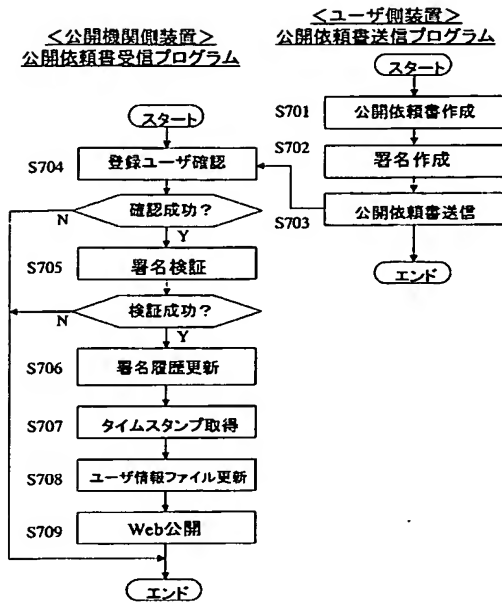
図6

署名履歴ファイル						
	604	605	606	607	608	609
	識別 番号	署名 番号	種別	前回署名 記録の ハッシュ値	文書の ハッシュ値	署名 or 受信した公開署名記録情報
601	Ver.1.0	1	受信	$H(S_0)$	—	$31 \parallel H(S_{31})$
602	Ver.1.0	2	送信	$H(S_1)$	$H(M_2)$	$\text{Sign}(2 \parallel H(S_1) \parallel H(M_2))$
603	Ver.1.0	3	受信	$H(S_2)$	—	$15 \parallel H(S_{15})$

ユーザ情報ファイル					
617 署名 番号	618 種別	619 相手情報	620 受信 署名 番号	621 公開 署名 記録	622 日時
610	0	新聞公開	新聞	—	—
611	1	受信	ユーザA@XXX.co.jp	32	$S_{31}$ 2002.1017.0816
612	2	送信	ユーザA@XXX.co.jp	—	—
613	3	受信	ユーザB@XXX.co.jp	16	$S_{15}$ 2002.1019.1550
614	4	送信	ユーザB@XXX.co.jp	—	—
615	5	新聞公開	新聞	—	$S_4$ 2002.1020
615	6	履歴送信	ユーザA@XXX.co.jp	—	—

【図 7】

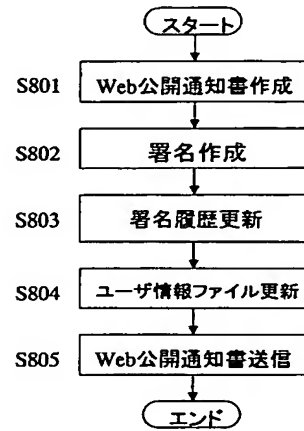
図 7



【図 8】

図 8

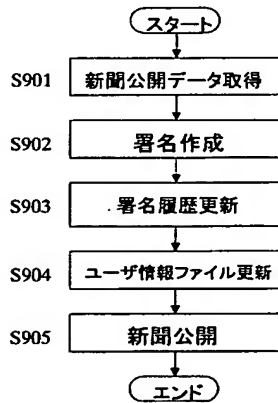
公開通知書送信プログラム



【図 9】

図 9

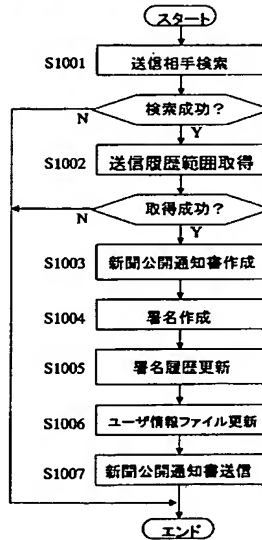
新聞公開プログラム



【図 10】

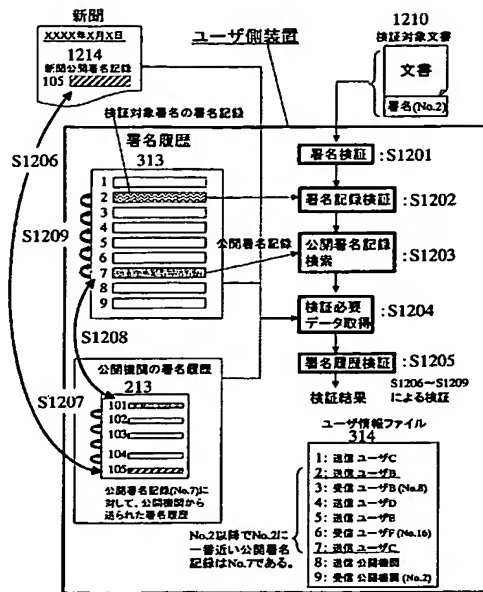
図 10

署名履歴送信プログラム



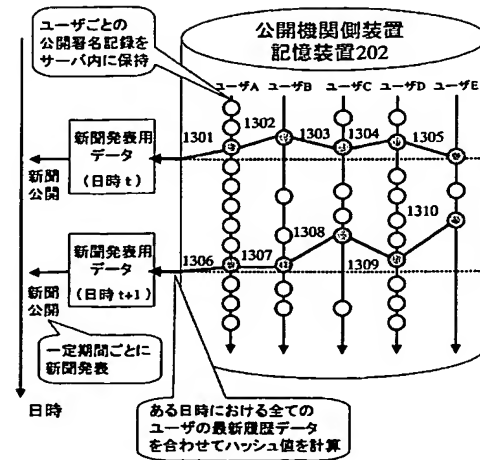
【図 1 1】

図 1 1



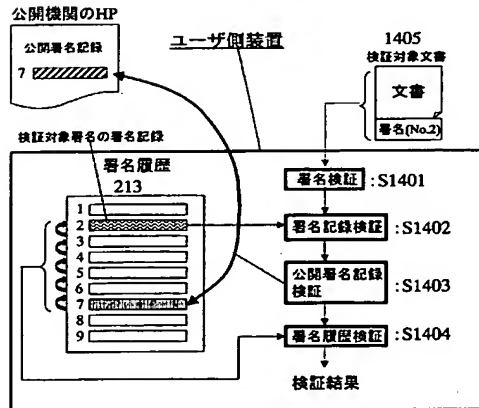
【図 1 2】

図 1 2



【図 1 3】

図 1 3



---

フロントページの続き

(72)発明者 伊藤 信治

神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

(72)発明者 工藤 康明

東京都江東区新砂一丁目 6 番 2 7 号 株式会社日立製作所公共システム事業部内

(72)発明者 別所 良治

東京都江東区新砂一丁目 6 番 2 7 号 株式会社日立製作所公共システム事業部内

Fターム(参考) 5J104 AA09